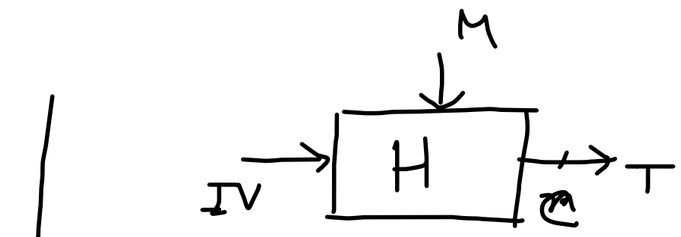
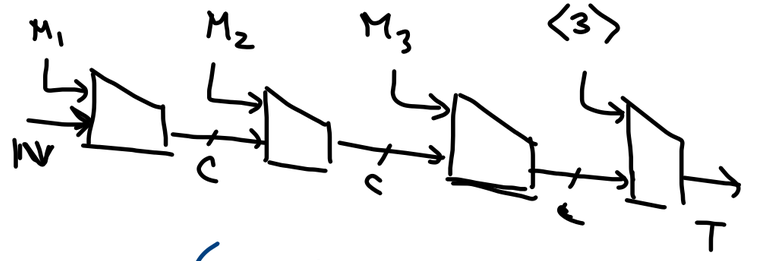
Joux's Multi-Collision Attack

Iterated Hash (MD hash) → Single collision requires $\approx 2^{c/2}$ queries

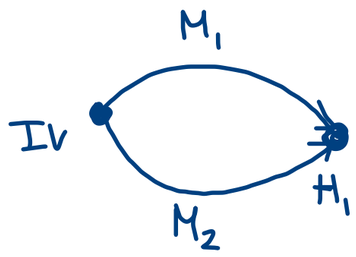
2^t Collision $\approx$ $2^t \cdot 2^{c/2}$ queries

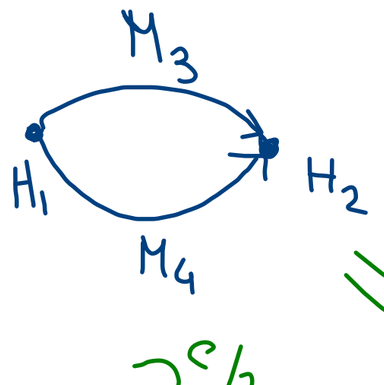




Graph based representation

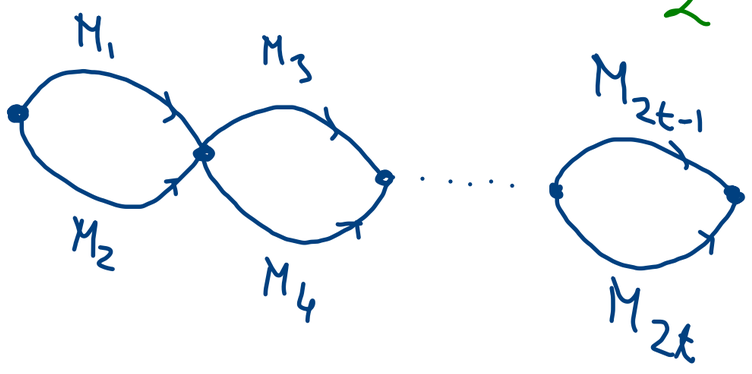
Birth day Attack ⇒





$2^{c/2}$

t-many Collisions



$H(M_1 M_3) = H(M_2 M_4)$
$= H(M_1 M_4) = H(M_2 M_3)$

$2^{c/2}$

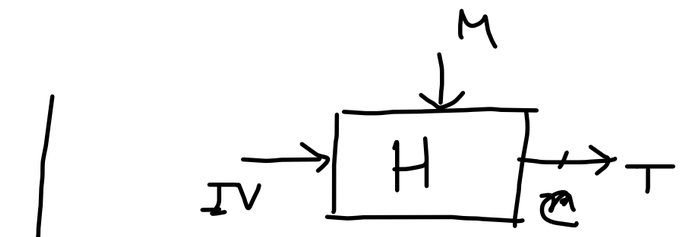
queries $\approx t \cdot 2^{c/2}$

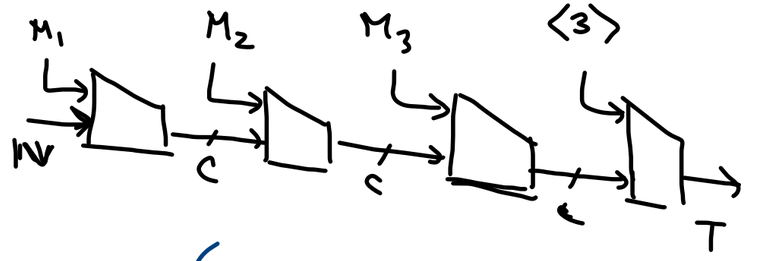
multi-collisions in the hash $= 2^t$

Joux's Multi-Collision Attack

Iterated Hash (MD hash) → Single collision requires $\approx 2^{c/2}$ queries

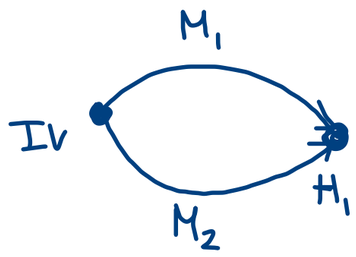
2^t Collision $\approx$ $2^t \cdot 2^{c/2}$ queries

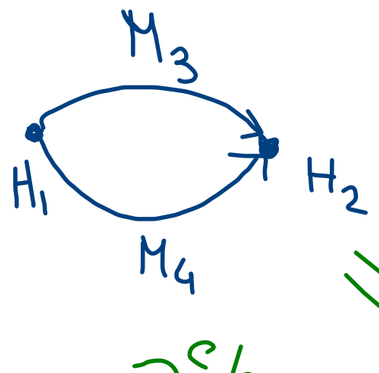




Graph based representation

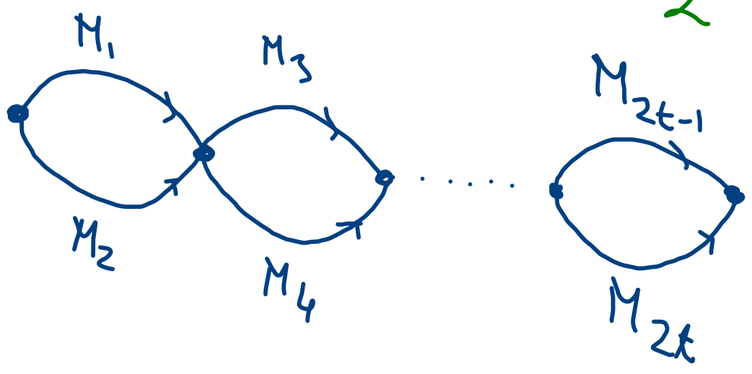
Birth day Attack ⇒





$2^{c/2}$

t-many Collisions



$2^{c/2}$

$H(M_1 M_3) = H(M_2 M_4)$
$= H(M_1 M_4) = H(M_2 M_3)$

queries $\approx t \cdot 2^{c/2}$

multi-collisions in the hash $= 2^t$

$$H(M) = \underbrace{H_1(M)}_{c} \,\|\, \underbrace{H_2(M)}_{c}$$

$\begin{cases} H_1 \rightarrow \\ H_2 \nearrow \end{cases}$ iterated hash function

#queries to find a collision $= 2^{c/2} \cdot 2^{c/2} = 2^c$ (Birthday attack)

How to mount an improved attack using Joux's Multi-Collision:

- Let us mount $2^{c/2}$ multicollision in H_1
- #queries for this =

$$H(M) = \underbrace{H_1(M)}_{c} \,\|\, \underbrace{H_2(M)}_{c}$$

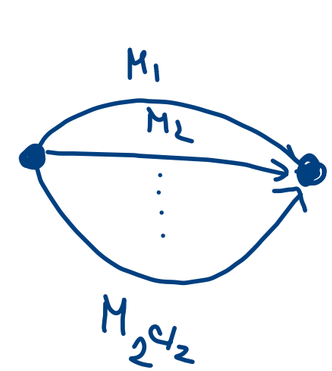
$\{$ $H_1 \rightarrow$ iterated hash function
$H_2 \nearrow$

queries to find a collision $= 2^{c/2} \cdot 2^{c/2} = 2^c$ (Birthday attack)

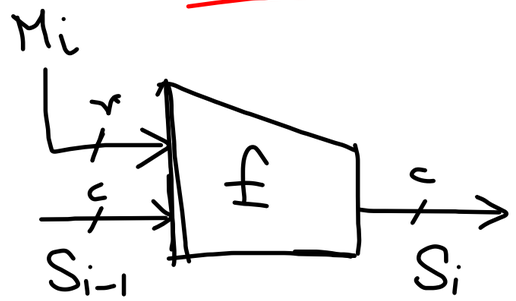
How to mount an improved attack using Joux's Multi-Collision:

- Let us mount $2^{c/2}$ multicollision in H_1
- # queries for this $= \frac{c}{2} \cdot 2^{c/2}$
- At least one collision in H_2. (Say M_i, M_j)
- Report (M_i, M_j) as colliding pair.

queries $= \frac{c}{2} \cdot 2^{c/2}$

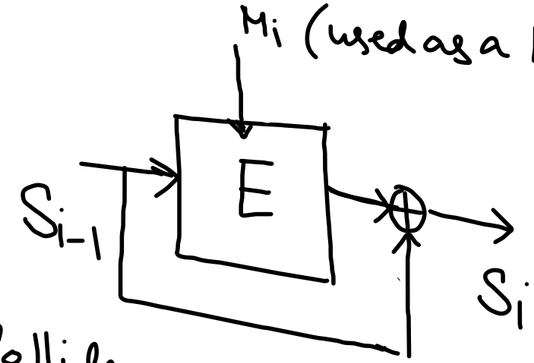


Constructing Compression functions

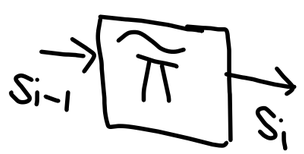


How to construct such function?

Davies Meyer Construction



— DM construction is Collision registance under ideal permutation Model.



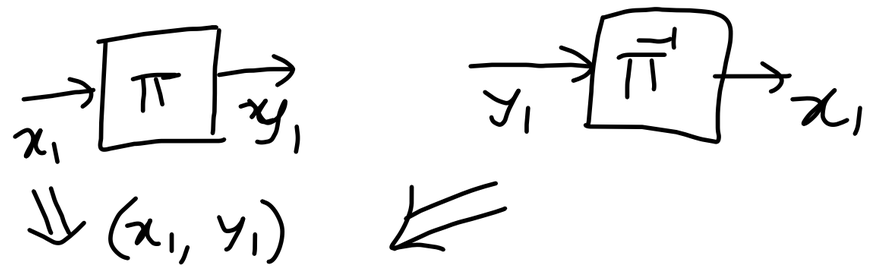
(x_1, x_2) Collides mean

$x_1 \oplus \tilde{\pi}(x_1) = x_2 \oplus \tilde{\pi}(x_2)$

$$Pr\left[\tilde{\pi}(x_1) \oplus \tilde{\pi}(x_2) = \rho\right] = \sum_{c^*} Pr\left[\tilde{\pi}(x_1) \oplus \tilde{\pi}(x_2) = \rho \mid \tilde{\pi}(x_1) = \rho^*\right] \cdot Pr\left[\tilde{\pi}(x_1) = \rho^*\right]$$

$$= \frac{1}{2^{c-1}}$$

$j \le 2^{n-1}$



$$\frac{1}{2^n - j + 1} \le \frac{2}{2^n}$$

$(x_1, \dots, x_q)$

$$\Pr[\exists\, i \neq j,\ y_i = y_j]$$

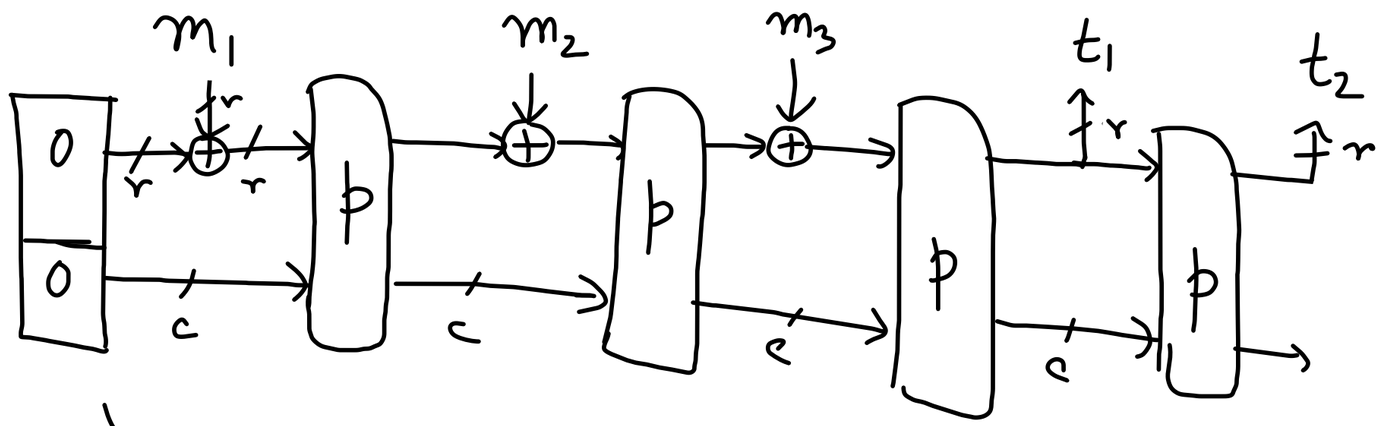
$$= \sum_{i,j} \Pr[y_i = y_j]$$

$$= \sum_i \sum_j \frac{1}{2^n - j + 1}$$

$$\le \binom{q}{2} \cdot \frac{2}{2^n}$$

DM is Collision resistance if $q < 2^{n/2}$

Sponge Mode Hash

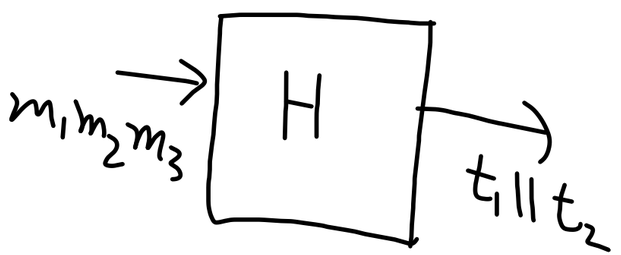


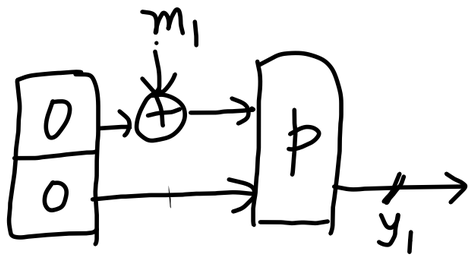
- $r + c = n$-bit state
- $r \rightarrow$ rate
- $c \rightarrow$ capacity

- CR upto $2^{c/2}$ queries

(Tight Security Bound)

- $p \rightarrow$ permutation on $\{0,1\}^{r+c}$



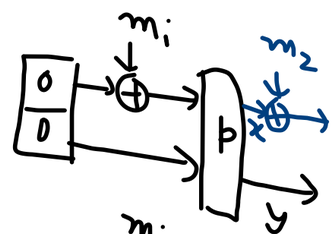


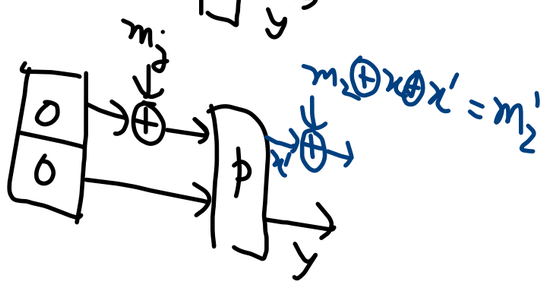
$\{r = c$

- Vary m_1^i & find $P(m_1^i \| 0) \mid_{i=1(1)q}$
- Check if $\exists$ a collision in y_1

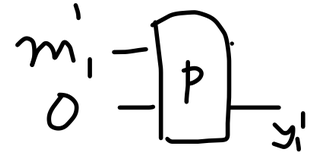
$Pr[\text{there is a Collision}] \leq \binom{q}{2} \cdot \frac{1}{2^c}$

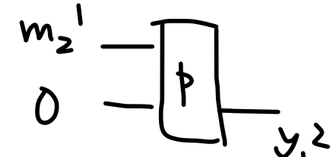
$q \approx 2^{c/2} \Rightarrow$ there is an collision with prob $\}$

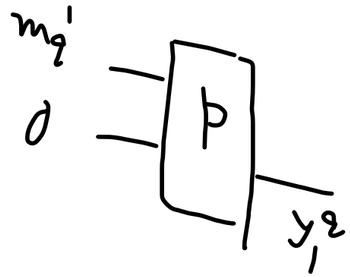




$(m_i \| m_2 \| *, \; m_j \| m_2' \| * \Downarrow) \rightarrow$ Collision



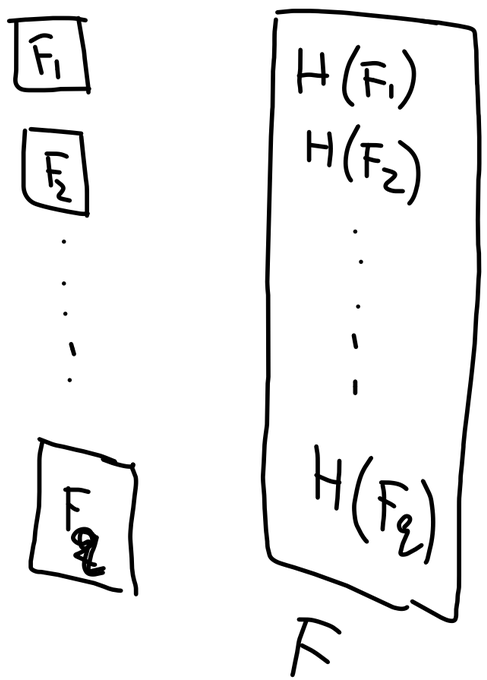




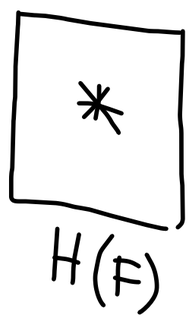
Applications

- How to verify whether your file has been modified or not?

Keep the hash & check.



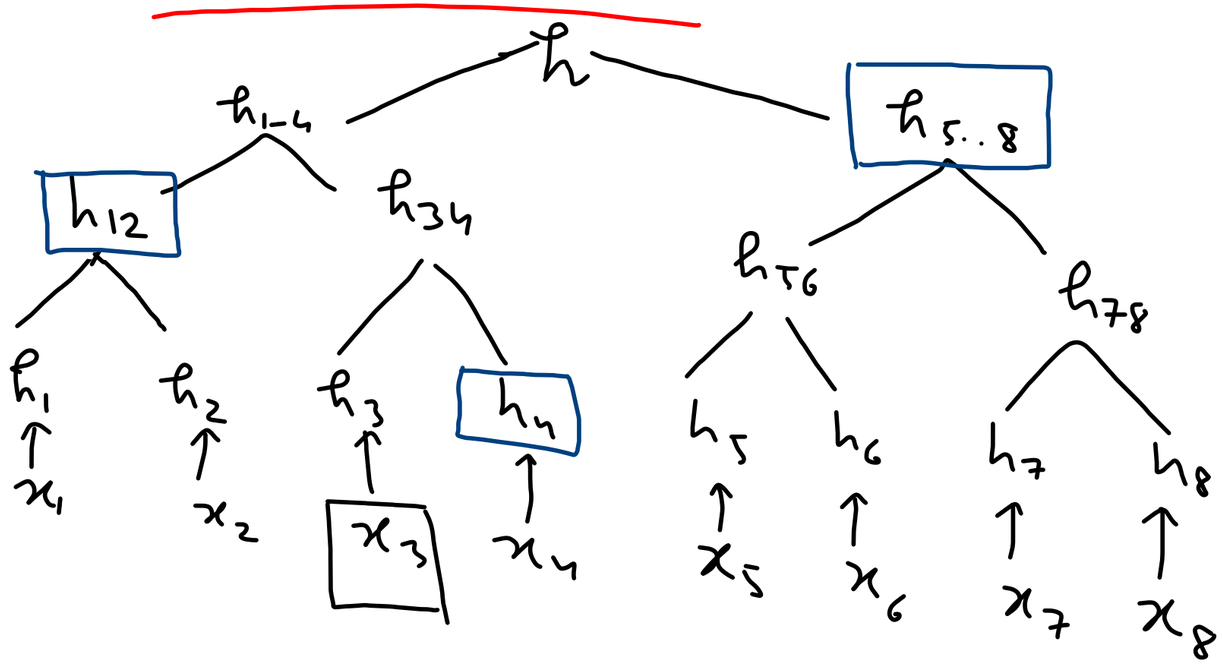
⇒ - Should be in a Read only memory
  - Size is very less



- Storage is very high
- Storage is low but all the files required.

Merkle tree

$h_{ij} = H(h_i \| h_j)$



ROM : h

{ How many files are required to retrieve x_3

⇓

3 file

ℓ file = $\log \ell$. many hash values }